LOGIN MODULE

September 14, 1999

SWSS Project

USER REQUIREMENTS

Table of Contents

1 INTRODUCTION

1.1 Purpose

Answer the question: “Why does this business process need to be automated?”

The SWSS application requires a login section in order to identify the user’s application identity, security level and a list of programs to which the user has update privileges.

1.2 Target Audience

Answer the question: “Who will want to and who will need to read this document, and why?”

This document is for the SWSS developers who are charged with creating a detailed design document for this module, as well as implementing the requirements listed herein. It will also be of interest to development staff charged with maintaining the SWSS automated system.

The following personnel may also be interested:

- SWSS Trainers
- FIA Help desk personnel
- SWSS advance users
- SWSS project staff tasked with developing the User’s guide
- Zone Children’s services specialists
- Assist operators/CIS clerks
- Policy Office Staff

2 MODULE NARRATIVE

2.1 Describe the business process in layman's terms. What sort of FIA staff are involved. What do they do? What forms do they deal with?

There is not a comparable process in the current programs of foster care, juvenile justice and adoption. Currently when staff need to find case information, they utilize the paper case file. There are not forms involved with the current process.

3 NAVIGATION FLOW

3.1 Screen Interaction

How should an automated system work from the user's perspective? What types of screens are needed and how does the user interact with those screens.

When the user accesses SWSS, the login screen is the first screen to come up. After the user types the login signon and password, the application flows to the Tickler section.

System Flow

How does the data entered in this module effect the system flow within this module (or beyond the scope of this module, if appropriate). For instance, in Legal, the legal status selected determines what functions are available to the user. Also in Legal, the petition type selected determines what functions are available to the user. This may not apply to every module in SWSS.

As noted above, the user's login determines the user identity, security level, and program type that the user accesses.

4 REQUIREMENTS LIST

The comprehensive (we hope) list of requirements derived from the original requirements, ensuing memos, emails, and test plan documentation.

4.1 Screen, Data, Out-of-Module, Output, Out-of-Module and Miscellaneous Requirements

The following requirements were derived from the original requirements documents written by policy staff for the SWSS project. Any ensuing memos, emails, or test plans regarding the project were also searched. It is intended to be a comprehensive list of all requirements pertaining to the Login module. Each individual requirement has a unique identifier; the two letter prefix identifies this particular module (LO = Login).

The list is to be used in a Requirements Traceability Matrix, which will be comprised of all the requirements for all the SWSS modules, so that the status of each requirement can be tracked and verified.

LO-1 SCREEN REQUIREMENTS:

LO-1.1 There must be a Logon screen.

LO-1.1.1 The following data items must be entered; i.e., they are required

LO-1.1.1.1 Username

LO-1.1.1.2 Password

LO-1.1.2 There must be a mechanism for the user to attempt to login to the application using the supplied Username and Password (an OK button).

LO-1.1.3 There must be a mechanism for the user to leave this screen without making a login attempt (a Cancel button). Choosing this mechanism, however, will prevent the user from entering the SWSS application.

LO-1.2 There must be a "Reset Password" screen. This screen will only appear when there is a need for the user to change his/her password.

LO-1.2.1 The following data items must be entered; i.e., they are required

LO-1.2.1.1 New Password

LO-1.2.1.2 Confirm Password

LO-1.2.2 There must be a mechanism for the user to save the new password data (An OK button).

LO-1.2.3 There must be a mechanism for the user to leave this screen without changing his/her password (a Cancel button). Choosing this mechanism, however, will prevent the user from entering the SWSS application.

LO-2 DATA EDITING REQUIREMENTS:

LO-2.1 "New Password" and "Confirm Password" fields of the "Reset Password" screen.

LO-2.1.1 These fields will only display the asterisk [*] character as the user types.

LO-2.1.2 The chosen password must not be case-sensitive

LO-2.1.3 The password must be from six to eight characters in length. Attempts to use more than eight characters are signaled with a beep and the extra characters are ignored. Passwords with a length of less than six characters are signaled with a warning message when the user presses the Tab key or tries to make an entry in another field.

LO-2.1.4 The user may enter any standard alpha or numeric character, as well as the underscore ("_") character into these fields. Use of the Backspace and Tab keys should also be permitted. All other keystrokes are forbidden and their illegal use is signaled with a warning message.

LO-2.1.5 The character combination entered in the "Confirm Password" field must match the character combination entered in the "New Password" field (the character case should not matter). If they don't, a warning message will be displayed. After the message is cleared, the user then has the option of either re-typing the password or he/she can cancel from the "Reset Password" screen.

LO-2.1.6 If the user enters a password that has already been used within the last three passwords changes, a message is displayed and the user is given the chance to try a different password.

LO-3 OUT-OF-MODULE REQUIREMENTS:

LO-3.1 COMMON ELEMENTS MODULE REQUIREMENTS:

LO-3.1.1 All modules, when dealing with Oracle database data[1], must detect error messages that indicate that the database connection has been severed. This disconnection could be caused by the database being "unavailable", the database "node" failing, or the network connection to the database failing.

LO-3.1.1.1 The module must attempt to automatically connect to another database "node" once this condition is detected. If all attempts to connect to any user accessible "nodes" fail, then a message must be displayed. This message must inform the user that the SWSS application is unable to connect to the database and must therefore shut down. The SWSS application must then terminate.

LO-4 MODULE REQUIREMENTS:

LO-4.1 A successful connection to the Oracle database with the provided username and password must allow the user to enter the SWSS application.

LO-4.1.1 A warning message must be displayed if the user enters their username or password incorrectly. This message must be displayed when the entered username/password *combination* cannot be found in the database. When the

[1] This includes reading, writing, and changing database data.

user acknowledges this message, the user must be given the opportunity to re-enter their username and password.

LO-4.2 If the SWSS Login module detects that the database is unavailable, the attempted database "node" is down, or the network connection to the database is severed, the module must then attempt to automatically connect to another database "node" (using the username/password combination entered by the user). If all attempts to connect to any user accessible "nodes" fail, then a message must be displayed. This message must inform the user that the SWSS application is unable to connect to the database and must therefore shut down. The SWSS application must then terminate.

LO-4.2.1 The SWSS Login module must support at least one and up to three possible database connection "nodes".

LO-4.3 Other circumstances can cause the display of information messages even if a successful connection has been made to the database. (details follow)

LO-4.3.1 If the current session is the first time a user is attempting to log into SWSS after his/her profile has been created, a message will be displayed and then the "Reset Password" screen will be displayed. This will force the user to change his/her password from its default setting before entering the SWSS application.

LO-4.3.2 If the current session is the first time a user is attempting to log into SWSS (after a Security Coordinator changed his/her password), a message will be displayed and then the "Reset Password" screen will be displayed. This will force the user to change his/her password from its current setting before entering the SWSS application.

LO-4.3.3 If a user logs in and it has been 90 days since the user has changed his/her password, they must be forced to change their password and a message must be displayed telling them to do so. The "Reset Password" screen will follow this so that the user is forced to update his/her password before gaining entry into the SWSS application.

LO-4.3.4 A message must be displayed if, in three past attempts, the user has correctly entered his/her username correctly but incorrectly entered his/her password. This message must inform the user that his/her SWSS username has been "locked" and that he/she must contact a Security Administrator to reset the password. Once the user has successfully logged into the SWSS application, the user must be given three new future chances to enter his/her username/password combination.

LO-4.4 The SWSS Login module must detect another instance of an active SWSS module and display a message informing the user that they must halt (close) the other active SWSS application before logging in. Once this message is acknowledged by the user (Ex.: by selecting an OK button), the new attempted instance of the SWSS application must terminate.

LO-4.5 Once the user has successfully connected to the Oracle database, some very basic information about the user is retrieved and stored in a file. This information will determine who the user claims to be and the application will do one of the following things based upon that information: (details follow)

LO-4.5.1 If the user is a Central Office Security Coordinator, a PROGRAM OFFICE OR P/DC user accessing the Payment Document Control utility or a Local Office Security Coordinator, then the user will be taken to the "SWSS Utilities" module. The login module will then shut down.

LO-4.5.2 If the user is not a Security Coordinator and the user is not a PROGRAM OFFICE OR P/DC user, then the user will be taken to the Ticklers module. The login module will then shut down. (See SC-4.9.7)

LO-4.5.3 Deleted

LO-4.6 If a user's account is inactive for 90 days, Login must refuse access to the SWSS and inactivate the user's account in the database; the user will have to request that their access be restored by a security coordinator.

LO-5 OUTPUT REQUIREMENTS:

LO-5.1 The Login module does not produce any printed output.

LO-6 MISCELLANEOUS REQUIREMENTS:

LO-6.1 Not applicable.

5 EXAMPLE OUTPUT

Gather and include the forms and letters generated by this module. If possible, mark up the examples to explain the data fields to show the source or whether or not it is required.
None.

6 DATA ELEMENT DESCRIPTIONS

A table of all the data elements entered within this module. For each item, describe its range of acceptable values. Designate items as being required for ASSIST, CIS, LICENSING or AFCARS (and any combination thereof).

ELEMENT NAME	**DESCRIPTION**	**TYPE - Alpha, numeric, A/N**	**SIZE**	**REQUIRED/ OPTIONAL/ CONDITIONAL**	**CIS/ASSIST AFCARS/ LICENSING output documents**
User name	Last name, first initial with number as necessary to make a unique user signon	Alpha / numeric	8 to 30	Required	Not applicable
Password		Alpha./ numeric	8 *	Required	Not applicable
To reset password					
New password		Alpha / numeric	8	Required	Not applicable
Confirm password		Alpha / numeric	8	Required	Not applicable

* currently the password can be more than 8 digits, however when it is reset it will need to be no less than 6 characters and no more than 8.

7 HELP MESSAGES

There are to be three levels of help available: Screen, which describes how the process for the current module is supposed to work, Context-Sensitive, which describes a particular data field on the screen, and Status Panel, which offer hints about the field or command button with the current focus.

SCREEN (Section or Module level. Offers an entry point to the big help file.)

CONTEXT-SENSITIVE ("F1", aka "detail")

STATUS PANEL MESSAGES (formerly known as "Field Level" and "Baby" before that.)

Module: Login

Field	New Message
Username	Enter user name
Password	Enter password
Cancel (cmd button)	Select to cancel
OK (cmd button)	Select to open SWSS

8 MODULE DEPENDENCIES

Login is dependent upon the User profile.

9 SCENARIOS

The requirements scenarios that call for data entered by this module. This is just a cross reference into the

10 TEST PLANS

The updated test plans written by the Program Office and/or the developer to verify the correctness of the finished application.

11 SOURCE MATERIAL

The following items are included for historical purposes only. The current requirements were derived from this source material, and are, in places, out of date, incorrect, or conflicting.

11.1 Original Requirement

LO-6.1.1 The user must be a Security Coordinator in order to Add or Inactivate staff profiles.

LO-6.1.2 When a Security Coordinator changes a profile's password, the user of that profile must be forced to change his/her password the next time he/she logs into SWSS.

LO-6.1.3 When a user logs into SWSS the first time after their profile is created, require that they change their password before allowing entry into SWSS.

11.2 Memos and E-mail

MEMORANDUM

To: Sue London, Director
SWSS Project

Date: October 14, 1999

From: Mary Ann Jensen, Consultant
SWSS Policy
Child and Family Services Administration

Subject: Login Module Documentation - Addendum 2

It is necessary to amend the Login Module Documentation Memo of October 1, 1999. After further discussion, it was noted that the following changes are needed:

LO-3.1 COMMON ELEMENTS MODULE REQUIREMENTS:

LO-4.1 A successful connection to the Oracle database with the provided username and password must allow the user to enter the SWSS application.

LO-4.1.1 A warning message must be displayed if the user enters their username or password incorrectly. This message must be displayed when the entered username/password *combination* cannot be found in the database. When the user acknowledges this message, the user must be given the opportunity to re-enter their username and password.

Remove requirement LO-4.1.2

LO-4.2 If the SWSS Login module detects that the database is unavailable, the attempted database "node" is down, or the network connection to the database is severed, the module must then attempt to automatically connect to another database "node" (using the username/password combination entered by the user). If all attempts to connect to any user accessible "nodes" fail, then a message must be displayed. This message must inform the user that the SWSS application is unable to connect to the database and must therefore shut down. The SWSS application must then terminate.

LO-4.2.1 The SWSS Login module must support at least one and up to three possible database connection "nodes".

LO-4.4 The SWSS Login module must detect another instance of an active SWSS module and display a message informing the user that they must halt

(close) the other active SWSS application before logging in. Once this message is acknowledged by the user (Ex.: by selecting an OK button), the new attempted instance of the SWSS application must terminate.

Add the following requirements:

LO-3.1.1 All modules, when dealing with Oracle database data[2], must detect error messages that indicate that the database connection has been severed. This disconnection could be caused by the database being "unavailable", the database "node" failing, or the network connection to the database failing.

LO-3.1.1.1 The module must attempt to automatically connect to another database "node" once this condition is detected. If all attempts to connect to any user accessible "nodes" fail, then a message must be displayed. This message must inform the user that the SWSS application is unable to connect to the database and must therefore shut down. The SWSS application must then terminate.

LO-4.3.4 A message must be displayed if, in three past attempts, the user has correctly entered his/her username but incorrectly entered his/her password. This message must inform the user that his/her SWSS username has been "locked" and that he/she must contact a Security Administrator to reset the password. Once the user has successfully logged into the SWSS application, the user must be given three new future chances to enter his/her username/password combination.

[2] This includes reading, writing, and changing database data.

cc: Sue Doby
Phil Rock
Nancy Presocki
Carol Kraklan

STATE OF MICHIGAN

FAMILY INDEPENDENCE AGENCY

MEMORANDUM

To: Sue London, Director
SWSS Project

Date: October 8, 1999

From: Mary Ann Jensen, Consultant
SWSS Policy
Child and Family Services Administration

Subject: SWSS/Staff Profiles Login Module Documentation - Addendum 1

It is necessary to amend the SWSS/Staff Profiles Login Module Documentation memo of October 1, 1999. At the time of the small group review of this module, the lockdown event log was not reviewed. A subsequent review of this event log determined that a new requirement was needed.

This requirement is that "Login must detect another instance of an active SWSS module and display a message informing the user that they must halt (close) the other active SWSS application before logging in." This instance normally occurs when the user is 'booted out' of SWSS because of a run time error.

Please let me know if you need additional information.

cc: Carol Kraklan
Phil Rock
Sue Doby
Nancy Presocki

STATE OF MICHIGAN
FAMILY INDEPENDENCE AGENCY

MEMORANDUM

To: Sue London, Director
SWSS Project

Date: October 1, 1999

From: Mary Ann Jensen, Consultant
SWSS Policy
Child and Family Services Administration

Subject: SWSS/Staff Profiles Login Module Documentation

We have carefully reviewed the User Requirements document on the SWSS/Staff Profiles Login Module and believe the September 14, 1999 document (printed on September 27, 1999) is complete as written.

Please let me know if you need additional information.

cc: Carol Kraklan
Phil Rock
Sue Doby
Nancy Presocki

STATE OF MICHIGAN
FAMILY INDEPENDENCE AGENCY

MEMORANDUM

To: Sue London, Director
SWSS Project

Date: March 31, 2000

From: Mary Ann Jensen, Consultant
SWSS Policy
Child and Family Services Adminstration

Subject: Log In, Security and Utility Module Documentation

Based on discussions and inclusion of the Payment Exception process (Payment Document Control utility), the above Modules required modifications. The following requirements have be added or modified and posted to on the Web:

1. LO requirements: LO-4.5.1 and LO-4.5.3.
2. Security requirements:
   - SC-4.1.1.1
   - SC-4.7.1
   - SC-4.9.6.1.1
   - SC-4.9.7
   - SC-4.12.1
3. Utility requirements:
   - UT-1.1.1.7 UT-1.2.1 UT1.2.2
   - UT-1.5.1.5 UT-1.5.1.5.1 UT-1.5.1.5.2
   - UT-1.5.1.5.3 UT-1.5.4.1 UT-1.8.2.2
   - UT-1.8.3.3 UT-3.4.1.1

These changes have been reviewed and approved. Please let me know if you need additional information.

cc: Carol Kraklan
Sue Doby
Phil Rock
Nancy Presocki

STATE OF MICHIGAN

FAMILY INDEPENDENCE AGENCY

MEMORANDUM

To: **Sue London, Director**
SWSS Project

Date: March 20, 2000

From: Mary Ann Jensen, Consultant
SWSS Policy
Child and Family Services Administration

Subject: Login Module Documentation – Addendum 3

It is necessary to amend the Login Module Documentation memos of October 1 and 14, 1999. After further discussion with development staff, it was determined that the following clarifications are needed:

1. LO-4.5.2 must be changed to state: If the user is not a Security Coordinator ~~or is a Security Coordinator with access to any other SWSS program (such as Foster Care, Adoption, etc)~~ and the user is not a PROGRAM OFFICE OR P/DC user, then the user will be taken to the Ticklers module. The login module will then shut down. (See SC-4.9.7)

2. Add a new requirement: LO-4.5.3 If the user is a PROGRAM OFFICE OR P/DC user accessing the Payment Document Control utility, then the user must be taken to the Payments-Document Control utility. The Login Module will then be shut down. (See PON-3.3, PON-3.3.1 and SC-4.9.7)

Please let me know if you need additional information.

cc: Nancy Presocki
Carol Kraklan
Phil Rock
Sue Doby

11.3 Test Plans

11.3.1 Test Plan Created by Policy

11.3.2 Test Plan Created by SWSS Development

Test Plan –SWSS Login

Matthew D. Miller

Process Accessibility

- All workers should have access to this process.

Process Functionality

- The process should detect if the worker enters an invalid combination of username and password. If that happens, a message box should inform the user of the error and give him/her a chance to try again. Also, if the SWSS_INI.INI file contains multiple database strings, the worker may also be offered the chance to try and connect to one of the other databases with the username/password combination that was entered.
- Upon successful entry of a valid username/password combination, the Login process should be shut down and the Tickler process should then be activated.
- The user should be able to leave the Login process if he/she cannot remember his/her username/password combination. This will prevent access to the SWSS system.

User's Guide
The SWSS application requires a security profile for every SWSS application User ID. Security profiles are a collection of information on the user, work location and requested access level. These profiles support system security and protect users from misuse of SWSS data. Profiles will be completed from completed FIA-60 forms.

Passwords represent a security risk and perhaps are the most vulnerable part of the security. SWSS has established the following requirements:

SWSS password length must be at least 6 characters long and no longer than 8 characters. Any combination of characters and/or letters are accepted.

Passwords are required to be changed every 30 days.

Passwords can not be reused until ## password change cycles.

Suggested password guidelines to follow:

- Don’ts use common words in proper or reverse spelling
- Don’t use your login name in any form (as is, reversed)
- Don’t use your first, middle or last name
- Don’t use your spouse’s or child’s name
- Don’t use easily obtained numbers such as telephone, street, social security number, birth date, etc.

User IDs will be locked out after 90 days of inactivity and removed after one year of inactivity.

12 OUTSTANDING ISSUES

12.1 The following items require a decision or some direction from Policy staff:

13 Attachment A: List of SWSS Module Prefixes